



Department of Energy

MANAGEMENT PROCEDURE NO. 5.3 LOS ALAMOS SITE OFFICE (LASO)



MP 5.3, Rev. 0

Effective Date:

10/13/2004

Approved:

LASO Manager

TITLE: SAFETY/DESIGN PROCESS INTEGRATION (CD-0 AND CD-1 PACKAGES)

1.0 PURPOSE

To describe the processes and expectations of the Los Alamos Site Office (LASO) relating to the integration of safety into design activities associated with new or major modifications to nuclear facilities as required by DOE O 420.1 "Facility Safety", and the development of Safety Basis (SB) documentation that meet the Title 10 Code of Federal Regulations (CFR), Part 830, Subpart B, (Rule) "Safety Basis Requirements" to support Critical Decisions (CDs) in the DOE Acquisition Management System as documented in DOE O 413.3 "Program and Project Management for the Acquisition of Capital Assets".

Note: This management procedure is limited to addressing safety-design integration during the pre-conceptual and conceptual design phases of a project lifecycle. This procedure will be expanded in future revisions/updates to address safety-design integration over the entire project life cycle.

2.0 SCOPE

This management procedure (MP) applies to LASO activities associated with the acquisition of capital assets involving design and construction of new or major modification to nuclear facilities that are within the purview of DOE O 413.3 requirements.

3.0 REFERENCES AND DEFINITIONS

3.1 References

- 10 CFR 830, Nuclear Safety Management
- DOE Order 413.3, Program and Project Management for the Acquisition of Capital Assets, dated 10-13-00
- DOE Order 420.1A, Facility Safety, dated 5-20-02
- DOE Guide 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE Order 420.1, Facility Safety, dated 3-28-00
- DOE Guide 421.1-2, Implementation Guide for use in developing Documented Safety Analyses to meet Subpart B of 10 CFR 830, dated 10-24-01
- DOE Guide 420.1-2, Guide for the Mitigation of Natural Phenomena Hazards for Nuclear Facilities and Nonnuclear Facilities, dated 3-28-00
- DOE Standard 3024, System Design Descriptions
- LASO MP4.2 - LASO Management Procedure for Document Review

3.2 Definitions

This section includes definitions of key terms associated with safety and design/project management functions. Definitions include the formal technical definition along with the specific reference from where the definition is taken and also a more practical, real-world explanation of the term and how it applies to the general area of safety-design integration. This approach is taken to facilitate common understanding of terminology and language.

Accident Analysis - Historically consisting of numerical estimates of the expected consequence and probability of potential accidents associated with a facility, Accident Analysis is a follow-on effort to the hazard analysis required only for facilities exceeding Hazard Category II thresholds and requiring documentation of the basis for assignment to a given likelihood of occurrence range in hazards analysis and performance of a formally documented consequence analysis [DOE-STD-3009-94]. Accident analysis focuses on the identification of safety class controls and defining environmental conditions, which will be used to drive design requirements for such controls.

Authorization Basis - Those aspects of the facility design basis and operational requirements relied upon by DOE to authorize operation [DOE-STD-3024-98] Authorization basis includes safety-basis as a subset, National Environmental Policy Act and environmental permitting and other documentation required to ensure safe, secure, environmentally compliant operations. 10CFR830 III, supplies further examples of Authorization Basis as including corporate operational and environmental requirements as found in regulations and specific permits, and, for specific activities, work packages or job safety analyses.

Construction - Any combination of engineering, procurement, erection, installation, assembly, or fabrication activities involved in creating a new facility or altering, adding to, or rehabilitating an existing facility. It also includes the alteration and repair (including dredging, excavating, and painting) of buildings, structures, or other real property. [DOE G 420.1-1, 3-28-00]

Critical Decision - A formal determination made by the Acquisition Executive and/or designated official at a specific point in a project life cycle that allows the project to proceed. [DOE M413.3-1]

Design Basis - Information that identifies the specific functions to be performed by a Structure, System, or Component (SSC) of a facility, and the specific value or range of values chosen for the controlling parameters as reference bounds of design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analyses (based on calculations and/or experiments) of the effects of a postulated accident for which the SSC must meet its functional goals. [10 CFR 50.2]

Document Safety Analysis (DSA) – Documented safety analysis means a documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety. A DSA is produced to one of 10 Safe Harbors as specified in 10CFR830 Subpart B, Appendix A.

Design Basis Accident (DBA) - An accident postulated for the purpose of establishing functional and performance requirements for safety SSCs. [DOE-STD-3009-94]. For new facilities and major modifications DBAs are used to support the basis for design specifications of safety SSCs. For existing facilities, DBAs correspond to evaluation basis accidents (EBAs) that could be used to judge the effectiveness and adequacy of existing safety SSCs to meet the environmental conditions created by the postulated accidents.

Functional and Operational Requirements (F&ORs) - Within Project Management, F&ORs translate program requirements into design products at the early stages of project development. Project technical requirements are translated from the mission need statement, to program requirements, to F&ORs, to design criteria, and finally documented in Facility/System Design Descriptions. In general terms, the F&OR will describe the processes and systems that must be included in a project to meet program requirements and fulfill program capabilities articulated in the project mission need statement.

Functional Requirement - In contrast to a F&OR in project management, in safety basis, *functional requirements define design requirements necessary to support the safety functions associated with SC and SS-SSCs. Functional requirements are typically associated with design criteria, e.g., facility structure must meet PC-3 seismic design loads.*

Hazard - A source of danger (i.e. material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation). [DOE 5480.23]

Hazard Analysis – The determination of material, systems, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with a process or activity. [DOE STD-3009-94]. Typical hazards analysis includes identification of hazards, scenarios, defense-in-depth, and potential safety significant controls, and identification of potential design basis accidents.

Performance Requirement - *Performance requirements are typically measurable criterion that is associated with functional requirements and are derived from the accident analysis for SC-SSCs based on the environmental conditions that are generated by postulated DBAs.*

Project - In general, a unique effort that supports a program mission, having defined start and end points, undertaken to create a product, facility, or system, and containing interdependent activities planned to meet a common objective or mission. [DOE O413.3]

Risk - The quantitative or qualitative expression of possible loss that considers both the probability that an event will occur and the consequences of that event. [DOE 5480.23]. From the safety analysis perspective, consequences are measured in terms of dose or exposure to various cohorts (e.g. public or workers). From a project management perspective, consequences are measured by impacts to program capabilities (mission need/technical project scope), or schedule, with consequences measured in terms of cost.

Safety Analysis - A documented process: (1) to provide systematic identification of hazards within a given DOE Operation; (2) to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and (3) to analyze and evaluate potential accidents and their associated risks. [DOE 5480.23] Safety analysis includes hazards and accident analyses and any other analysis required to support evaluation of adequacy of controls or compliance with requirements.

Safety Basis – Safety basis means the documented safety analysis (DSA) and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment. Safety basis is comprised of a Documented Safety Analysis (PDSA for design/construction phases). Technical Safety Requirements (TSRs) (for operational facilities), and the Safety Evaluation Report (SER) as well as any documents which amend the safety basis such as approved USQs (if applicable).

4.0 RESPONSIBILITIES

4.1 LASO Manager

- 4.1.1 Review and approve all LASO management procedures.**
- 4.1.2 Approval of Safety/Authorization Basis documentation for LANL facilities.**
- 4.1.3 Review recommendations and give final approval for technical issues relating to quality assurance.**
- 4.1.4 Ensuring all LASO operations and requirements that fall within the scope of DOE Orders 413.3 and 420.1A are in compliance with the Order requirements.**
- 4.1.5 Ensuring that all exemptions to design requirements are accepted and approved by DOE prior to their implementation.**
- 4.1.6 Reports directly to the Administrator, National Nuclear Security Administration and has line accountability for contract management of all site program/project execution.**
- 4.1.7 Ensuring adequate LASO resources are in place to support execution of activities that fall within DOE Orders 413.3 and 420.1A**

4.2 LASO Senior Authorization Basis Manager

- 4.2.1 Participates in the development, review, approval, routine updating, and maintenance of this Management Procedure (MP).**
- 4.2.2 Ensures appointment of LASO SABB staff resources for the activities described in this MP as required to meet 10 CFR 830 requirements in accordance with the SABB review procedure.**
- 4.2.3 Establishes and maintains routine collaboration and interface with LASO Assistant Manager for Project Management regarding effective integration of Safety and Design activities.**

- 4.2.4 Provides guidance and expectations on Safety Basis (SB) documentation required to support CD activities.
- 4.2.5 Reviews exemptions to design requirements, evaluates impact on safety, and defines residual risk on behalf of LASO Manager, for submittal to DOE for exemption request approval.
- 4.2.6 Provides timely review and approval to safety basis documentation developed in support of CD activities associated with the design and construction of new or major modifications to nuclear facilities.
- 4.2.7 Identifies resource requirements needed to fulfill LASO responsibilities within assigned functional area and communicates said requirements to LASO Manager.
- 4.3 **LASO Assistant Manager for Project Management**
 - 4.3.1 Participates in the development, review, approval, routine updating, and maintenance of this Management Procedure (MP)
 - 4.3.2 Ensures assignment of LASO Federal Project Directors for all projects under the purview of DOE Order 413.3, subject to 10 CFR 830, Subpart B.
 - 4.3.3 Establishes and maintains routine collaboration and interface with LASO SABB Manager regarding effective integration of safety into design activities, and the review/approval of SB documentation in support of projects under the purview of DOE Order 413.3, subject to 10 CFR 830, Subpart B requirements.
 - 4.3.4 Establishes and maintains routine collaboration and interface with Contractor (e.g., LANL) personnel supporting the preparation of design and documentation in support of CDs.
 - 4.3.5 Ensures overall implementation of the acquisition management system including the oversight of all Planning, Programming, Budgeting, and Evaluation (PPBE) activities associated with the integration of safety into design on behalf of LASO Manager.
 - 4.3.6 Identifies resource requirements needed to fulfill LASO responsibilities within assigned functional area and communicates said requirements to LASO Manager.
- 4.4 **LASO Federal Project Director (Office of Project Management Staff)**
 - 4.4.1 Establishment of Integrated Project Team for assigned projects, including integration and coordinating support from LASO SABB.
 - 4.4.2 Being cognizant and knowledgeable of 10 CFR 830 and DOE Order 420.1A requirements.
 - 4.4.3 Ensuring assigned projects are developed and implemented in compliance with applicable CFR and DOE Order requirements
 - 4.4.4 Utilizing the processes and procedures outlined in this MP as well as other methodologies to facilitate integration of design and safety functional areas for assigned projects.
- 4.5 **LASO Staff - Safety Authorization Basis Team**
 - 4.5.1 Participating as active members in LASO Integrated Project Teams necessary to support development and execution of design and

construction activities to ensure compliance with 10 CFR 830 and DOE Order 420.1A requirements.

4.5.2 Executing LASO SABB responsibilities IAW the requirements contained in this MP.

4.5.3 Being cognizant and knowledgeable of DOE Order 413.3 requirements.

5.0 PROCEDURE

This section defines the process and expectations to ensure compliance with DOE O 420.1A, DOE O 413.3, and 10CFR830 Requirements, and more specifically the integration of safety and design functional activities. This process starts with a description of the DOE Acquisition Management System, followed by a general description summary of safety/design objectives derived from Regulatory drivers, a general description of the safety/design integration process, and finally more detailed outlining of expectations related to specific information/documentation (including SB documentation) needs to support the various CDs in the DOE acquisition management system for nuclear facilities. A discussion on the integration of design and SB documentation, with environmental (i.e., NEPA) documentation is also presented. The SB documentation for nuclear facilities include the Documented Safety Analysis (DSA), the Technical Safety Requirements (TSRs), and Safety Evaluation Report (SER).

5.1 DOE Acquisition Management System Summary

DOE has established a project acquisition management system that is designed to establish a management process that translates project needs (missions) into reliable and sustainable facility and SSCs that meet the mission requirements. The acquisition management system is organized by project phases and critical decisions (CDs). The project phases represent a logical maturing of stated mission needs into well defined technical, SSCs, safety, and quality requirements; while, the CDs represent a formal determination or decision at a specific point in a project phase that allows or authorizes the project to proceed to the next phase. A brief summary of the project phases and their relationship to CDs follows. Figure 1 illustrates the DOE acquisition management system (DOE O 413.3) in which such relationships are explicitly identified.

- a. **Project initiation** also known as the pre-conceptual planning phase focus on program's strategic goals and objectives, with a goal to clearly develop the project Mission Need Statement in terms of required capability (both in terms of mission functional and performance requirements). Approval of the mission need is the first CD (defined as CD-0).
- b. **Definition phase** also known as the conceptual design phase focus on the evaluation of alternative concepts (functions and capabilities) through the use of system engineering or similar techniques to determine the optimum life cycle cost that meets the required performance, scope, and schedule. Approval of alternative selection and cost range is accomplished through the CD-1. The definition phase serves to define the conceptual design phase. Both the project initiation and definition phases form part of what is also known as the overall project planning phases as indicated in Figure 1.
- c. **Execution phase** includes the preliminary, final or detail design, and construction phases. The preliminary design phase culminates with the development and approval of the Performance Baseline (CD-2) that defines

the required capability, scope, cost, and schedule for the project. The final or detail design phase is completed with start of construction activities is authorized through CD-3. The execution phase is completed when all the required capabilities are implemented to meet the functional and performance requirements of the project, including the availability of operational resources and trained personnel to execute the mission needs. CD-4 defines the approval of the project completion.

- d. **Mission phase** represents the operation phase of the facility. This phase starts with the authorization of operations by the approval of the SB documentation (i.e., DSA, TSRs, and SER) and a successful DOE operational readiness review (ORR).

The CDs are designed to function as hold points to demonstrate sufficient development and readiness to proceed onto the next phase of the project. DOE Order 413.3, Attachment 4, lists the major deliverables for each CD over the project lifecycle. CDs are achieved through the implementation of the Energy Systems Acquisition Advisory Board (ESAAB). Different ESAAB's are established at Site Office or Headquarters levels, depending on the size (\$ value) of the project.

In general, within the DOE/NNSA project management system, the following areas are reviewed and evaluated in order to assess a project's readiness to proceed during each CD:

- Mission Need and Project Goals
- Management Systems, Controls and Planning
- Acquisition Strategy
- Security and Safeguards
- Technical Scope
- Cost Estimates and Funding
- Schedule
- Risk and Contingency Management
- Environment, Safety and Health
- Energy Conservation
- Waste Minimization and Pollution Prevention

Over the course of the project life cycle each of these areas are developed in more detail as additional design and technical analysis is completed. All project management activities conducted at LASO are executed in compliance with Order 413.3 requirements. As the specific intent of this management procedure is to focus on integration of safety into design, detailed requirements for the full suite of project management related activities over the project life cycle are not contained in this document. Rather, the primary focus is only on those project management activities critical in the integration of safety and design. For additional detailed explanation of project management activities, see DOE M 413.3-1. Additionally, the "[Independent Review Process for Construction and Related Programs](http://hq.na.gov/NA-54)" dated March 2004, available through the NA-54 website at <http://hq.na.gov/NA-54> provides lines of inquiry for the various project critical decisions that serve as a useful guide and tool.

5.2 General Safety/Design Integration Objectives

The major general objectives associated with the integration of safety into design activities are to:

- 5.2.1 Ensure an effective coordination and integration between LASO Office of Project Management (OPM) and Safety Authorization Basis Team (SABT) activities in order to ensure timely compliance with 10 CFR 830 and DOE O 413.3 requirements.**
- 5.2.2 Ensure that a safety analysis is performed at the earliest practical point in the conceptual or preliminary design phases of a project so that required attributes of facility SSCs can be specified in the detailed design as required by DOE Order 420.1A. The safety analysis consists of a hazards and accident analysis (for HC-2 nuclear and high-hazard non-nuclear facilities), such analyses must be conducted as early as possible (i.e., conceptual design phase) to identify all potential safety class and safety-significant structures, systems and components (SSCs)**
- 5.2.3 Ensure integration of SB development and project management activities in an iterative manner over the project lifecycle to effectively demonstrate compliance with 10 CFR 830 and DOE O 413.3 requirements. This requires continuous coordination between the facility design process and the development of facility safety analysis/documentation to ensure that final design meets the mission requirements and includes required safety features and systems to ensure implementation of Integrated Safety Management (ISM) processes.**
- 5.2.4 Integrating the design and safety basis activities through use of a systems engineering approach tailored to the specific needs and requirements of each project.**
- 5.2.5 Ensure that new or major modifications to HC-2 and HC-3 nuclear facilities incorporate the concept of Defense in Depth into the facility design process, with the objective of providing multiple layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment and protect workers.**
- 5.2.6 Ensure that the design and construction shall incorporate design requirements identified in DOE O 420.1A for all new or major modifications to non-reactor nuclear and non-nuclear facilities in a graded manner to SSCs identified as safety-class, safety-significant, or defense-in-depth controls based on the safety analyses performed for the facility. Exemptions to any specific design requirement identified by the Order shall be evaluated to determine the impact on safety, and be approved before implementation of such deviation(s).**

5.3 Integration of Safety Into Design In Support Of Critical Decisions

This section is intended to describe the processes related to integration of safety and design functional areas. The basic approach taken is to describe both the project management and SB development activities, along with their interfaces including with those associated with NEPA documentation (environmental documentation), during each of the major phases of the traditional project lifecycle. Figure 2 depicts the general processes used by NNSA-LASO to ensure

the integration of safety/authorization basis development and design activities over the life of a typical construction project, it also identifies the various SB documentation used to support the CDs, and their integration with the facility and systems design descriptions (FDDs/SDDs); the later are part of the design documentation.

This section further describes the purpose or intent of each of the CDs, followed by a description of project management related activities and expectations in those areas concerning safety and description of safety-basis related activities and deliverable expectations, complete with a practical example that describes safety basis and project management considerations at each phase of development. The examples provided are intended to function as an aid in communicating the specific safety-design integration goals/objectives at that particular phase of the project.

One fundamental objective of this section is to communicate the DOE Project Management Critical Decision (CD) processes for non-project management personnel, and similarly, describe the general safety basis development processes for non-Safety/Authorization Basis personnel. An example will be used to illustrate the integration of safety into the design process.

Identification of the complete format and information needs for each of the CDs is provided in DOE O 413.3, DOE M 413.3-1, and other program-specific guidance as issued by the Lead Program Secretarial Officers with DOE and NNSA.

The process/procedures outlined in this document are intended to describe fundamental safety basis deliverables and expectations at each phase of project development irrespective of project management/acquisition approach. In other words, this document describes general processes and expectations of safety basis development necessary to support engineering design and project development maturation without concern to contracting type or acquisition strategy. Fundamentally, there are minimum safety basis development expectations necessary at each stage of design development. How fast or slow one proceeds with engineering development will drive the speed at which safety basis development must occur, regardless of the acquisition approach implemented. The key point is understanding minimum safety basis development expectations at each stage of project development and ensuring that the procurement approach selected allows for achievement of these minimum safety basis requirements and expectations.

5.3.1 Critical Decision 0 - Approve Mission Need

Purpose: The fundamental purpose/intent of CD-0 is to obtain approval of the project Mission Need Statement from the DOE/NNSA Acquisition Executive. Approval of the mission need is the authorization to develop alternative concepts and project functional requirements. This decision also approves use of operating expense funding to perform the conceptual design activities and produce the deliverables described in paragraph 5.3.1.4 below.

Project Management: From the project management point of view, the Initiation (CD-0) Phase of a project begins prior to the identification of a capital asset need. During this period, normally referred to as pre-conceptual planning, the responsible NNSA/DOE program office element identifies a performance gap

between its current and required capabilities and capacities to achieve the goals articulated in DOE, NNSA and LANL strategic plans. A mission need is the translation of this gap into project functional requirements that cannot be met through other than material means (a capital project).

The outcome of this phase leads to the development of a request for Critical Decision 0, Approve Mission Need as the initial step in the acquisition process. Mission need requirements should not be defined in equipment, facility, or other specific end item, but in terms of the mission, purpose, capability, schedule and cost goals, and operating constraints. That is, the primary focus of planning at this stage is development of a mission need statement that includes at a minimum, the following:

- a description of the performance gap between current and required capabilities, or regulatory requirements requiring action;
- analysis used to identify the gap or shortfall;
- description of the importance of mission need and impact if not approved;
- constraints and assumptions;
- resource planning/feasibility cost estimate/schedule/milestones; and
- a development plan including alternative actions to be considered

Pre-conceptual planning essentially results in the development of a mini-baseline for conceptual design activities during the next phase of the project. As such, sufficient information must be provided to validate the projected cost, schedule and technical scope associated with the conceptual design effort for the proposed project.

As limited technical analysis has been completed, most planning represents strategies for accomplishing the various tasks (i.e. NEPA strategy, Safety Basis Strategy, Acquisition Strategy, etc). The outcome of pre-conceptual planning leads to the development of a request for Critical Decision 0, Approve Mission Need as the initial step in the acquisition process. Specific deliverables that make up the CD-0 Request are described in section 5.3.1.4.

***Example:** An example of a mission need statement might be the production at LANL TA-55 (PF-4) of two qualified RTGs for the NSA space program, and with sufficient capability to support the storage and process enough radioactive material to produce two additional RTGs.*

The example provided above will be expanded upon in this MP to demonstrate how design and safety-basis documentation is developed as the project evolves, highlighting specific issues and/or considerations important to integration of the two functions.

5.3.2 Safety Analysis Considerations

There are no specific safety analysis or documentation deliverables during the initiation or pre-conceptual planning or initiating phase. However, at CD-0 (end of the initiation phase), it is expected that some preliminary safety analysis and documentation can be initiated that can be used in support of the mission need statement. Typical information and preliminary safety analysis for this pre-conceptual planning phase include:

- a. Initial identification of major facility hazards based on mission needs and objectives (from established project mission functional and performance

requirements). Characterize major hazards that will drive design requirements.

Example: From the example mission statement we can determine a major nuclear dispersal hazard associated with meeting the mission functional and performance requirement for which one can begin to formulate initial Material -at-Risk (MAR) hazard assumptions. That is, it is known that at least two “qualified” RTGs and the capability to support two additional ones, tell us that we need the ability to store and process at least 2 kg of type MT-83 (mostly ^{238}Pu material in an oxide form) at the facility (for illustration purposes, assume that a new facility is to be built to support this mission, and that each RTG contains approximately 500 g ^{238}Pu).

- b. Establish initial hazard categorization based on facility radiological hazards using DOE-STD-1027 inventory thresholds, for chemical hazards use NNSA approved or endorsed specific categorization criteria for non-radiological facilities, e.g., based on ERPG values.

Example: The quantity of ^{238}Pu from the hazard identification (2000 g of type MT-83 oxide) is significantly larger than the threshold for a HC-2 facility (3.6g of ^{239}Pu) or operation from DOE-STD-1027 Appendix A. Thus, the facility and operations required to support the RTG program is initially categorized as HC-2, based on the total inventory needed to support the mission.

- c. Establish early preliminary design requirements to meet mission needs, based on potential unmitigated consequences from the process or facility.

Example: Since the facility and process categorization is HC-2, and because of the potential source terms (based on the 2 Kg of MT-83 material in assumed releasable (but as yet not fully determined) form which is roughly about half metric tone of ^{238}Pu equivalent) and location at LANL with respect to the maximum offsite individual (MOI) (i.e., within 1 km of the site boundary), the unmitigated consequences for major accidents (fire, Seismic) will likely (qualitative determination) exceed the DOE Evaluation Guidelines (EG) of 25 rem to the MOI. Based on the fact that the EG could be exceeded, a set of preliminary design requirements can be established at least for the facility structure, e.g., PC-3 seismic loads.

- d. Initiate identification of applicable design criteria for the facility. Facility safety requirements shall be derived from DOE O 420.1A for nuclear facilities. Identify any preliminary design exemptions, especially facility safety design requirements.

Example: DOE O 420.1 identifies facility safety design requirements (including codes and standards) in the areas of nuclear safety design, criticality safety, fire protection, natural phenomena hazards mitigation, and system engineering for all major modifications and new facilities. As indicated by DOE- O 420.1, nuclear safety design requirements shall be guided by safety analyses and thus, as the safety analysis progresses the nuclear design requirements are identified s much as is reasonably feasible at that point in time.

Independent of the results of the safety analysis there are several design requirements identified for nuclear facilities, these include among others the design with the objective of providing multiple layers of protection to prevent or mitigate to potential release of radioactive material to the environments. All activities associated with potential dispersible radioactive material shall be confined so as to prevent the spread or release of radioactive material to the working areas and to the environment.

Design requirements and criteria can then be derived from DOE O 420.1; any exemptions to DOE O 420.1 requirements need to be identified at this stage. For example, the project may identify the need to take an exemption to the seismic design criteria for HC-2 facilities with the potential to exceed the EG. That is, instead of designing the facility structure to survive PC-3 seismic loads; it is being proposed, that the facility meet only PC-2 seismic loads, because the proposed location of the facility is unstable seismically.

- e. Initiate analysis of impact on safety for any safety design requirements exemptions

Example: At this stage of the project planning process, a seismic evaluation is planned to determine the maximum seismic capability that the site will provide to the facility structure. A safety analysis is also planned to determine the impact of seismic events including seismic induced fires and nonseismic fires on the future of this facility. Note that completion of this analysis at this time is not required, only the initiation of planning for this activity as necessary to identify/acquire the requisite expertise and resources to perform this task.

- f. Establish and demonstrate compliance with site selection criteria

Example: At this stage an evaluation of the impact of the facility sitting on public, and adjacent facilities and worker personnel is started to determine if adequate protection can be provided to both workers and public. This evaluation will be used to determine if the proposed operations will adversely impact adjacent facilities and operations, or vice-versa.

- g. Preliminary identification of major facility safety SSCs, i.e., major defense-in-depth controls to provide safety, based on major hazards. At this stage we may not know if such SSCs will perform safety-class functions.

Example: It is clear that the in order to meet DOE O 420.1 requirements with respect to defense-in-depth and based on the above mentioned conclusions with respect to hazard identification, hazard categorization, etc., that the major facility SSCs (not inclusive) will be facility structure and confinement capability, including the need for fire rating (minimum 2 hr fire rating for the external wall of the facility per DOE design requirements)

- h. Initiate preliminary safety function definitions for preliminarily identified safety SSCs

Example: Based on the above-identified safety SSCs, safety functions are identified. For example for the facility structure, some of the safety functions will be:

- support confinement of potential airborne radioactive materials
- provide structural integrity, including seismic capability to support all safety SSCs attached or located inside the facility
- Prevent fire compromise of the external walls.

i. It should be noted that there are some complexities inherent in doing a major modification in an existing facility. The following are considerations:

- The existing DSA needs to be evaluated relative to its ability to support and integrate with major modification. For example, if a major modification requires the identification of new safety SSCs (Safety Class, Safety Significant) then a consideration is how to integrate the new systems with the existing DSA and TSRs. At some point in the PDSA cycle, the major modification will become operable and must therefore be part of the facility TSR envelope.
- Another consideration when performing a major modification would be the extent to which existing safety SSCs would be affected or modified. Operability of the SSCs would have to be assured, or compensatory measures defined if the facility is to be operable during the major modification and approved by DOE. Alternatively, argument could be made to defend placing affected portions or all of the facility into a safe configuration during the modifications. If a facility is to remain operational during the modifications the transient hazards must be analyzed with effective safety controls defined and verified. Following major modifications Readiness reviews (RAs) or an ORR must be performed to ensure the formal and effective implementation of safety controls. These RAs/ORRs may need to be phased to allow for program mission flexibility (but may become more complex when phased).

j. In support of the formal CD-0 request, the above information described in sub-elements 1-8 above, are used to feed the development of a plan to perform the safety and hazards analysis activities during the conceptual design phase. Keep in mind that CD-0 authorizes the use of operating expense funding to perform conceptual design and other activities necessary to support the next Critical Decision, CD-1, which establishes a preliminary baseline range and authorizes start of preliminary design activities. Safety-basis development activities at CD-0 are described in summary fashion in what is normally titled a Pre-Conceptual Project Plan. This plan, presented in concert with the mission need statement, represents a baseline agreement for what will be developed during the next phase (conceptual design phase) of the project, who is responsible, what it will cost, and how long it will take. There is no specific format for a pre-conceptual Project Plan, and the details will vary depending on project complexity and size, yet it must communicate the basics of what, who, when, and how much will it cost.

Summary of Safety Analysis Considerations at CD-0:

At the end of the pre-conceptual (or initiation) planning phase signaled by receipt of an official Critical Decision 0 in the form of a memorandum from the DOE/NNAS Acquisition Executive, the preliminary documented safety analysis (PDSA) or preliminary (design) hazard analysis for this project phase is started. No formal safety basis documentation is required to be submitted for CD-0 - Mission Need Approval. However, the following safety basis information should be known/available to support the planning for Conceptual Design Phase Activities:

- Initial identification of major facility hazards based on mission need
- Initial hazard categorization based on preliminary facility hazards
- Whether there is a potential for challenging or exceeding DOE EG at the MOI, and thus the potential need for SC-SSCs
- If there is a potential for challenging or exceeding the EG, preliminarily determine if the facility will be required to be SC-SSC, and what safety functions will the structure provide. Also if possible, determine preliminary set of functional requirements for the SC-SSC
- Determine preliminary set of design requirement exemptions for any preliminarily identified SC-SSCs, from those design requirements identified in DOE O 420.1 and its implementation guides.
- Initiate evaluation (planning) of impacts (e.g., on safety of workers, public) of exemptions to design requirements, if any
- For major modifications, a general understanding of the potential impacts to existing safety/authorization basis for the facility along with initial planning for safety-basis development and integration as part of the proposed project should be available.

As indicated in Table 1, ISM elements are integrated into project planning phase (i.e., pre-conceptual design (or initiation) and conceptual design (definition) phases. The ISM activities associated with defining the work (design baseline), design basis/analyze the hazards, develop design requirements, and perform design work (facility level) that were briefly discussed above are initiated but are not required to be completed during CD-0.

5.3.3 Deliverables: A CD-0 package consists of the following:

1. Justification for Mission Need document (Reference DOE M413.3-1, Chapter 4)
2. Acquisition Strategy (e.g., design-bid-build, design-build, acquisition decision process, factors that will affect the decision, strategy to obtain and use PED funding, etc.)
3. Pre-conceptual Planning Summary - normally addressing at a minimum:
 - statement of mission need,
 - description of project (including location, purpose/function, goals, identify alternative concepts, etc.),
 - minimum project technical/functional requirements (include design documentation package planning and preliminary design information available for alternative concepts, demonstrate linkage with requirements and mission, system engineering planning, etc.). Note

that project functional requirements are not the same as the functional requirements for safety SSCs).

- resource capability (include identification or strategy to obtain the required capabilities to support the mission) ,
- proposed cost/schedule (including durations for design and construction phases, preliminary funding profile, preliminary CD-1 and CD-2 request dates versus budget cycle milestones, etc.),
- conceptual planning/acquisition (e.g., schedule, cost-budget/funding sources, who will prepare the CDR),
- preliminary safety analysis or determination (define safety objective and constraints, *start* the safety analysis and documentation activities identified in section 5.3.1.3 for each alternative conceptual design alternatives, in other words, what is the plan to complete safety analysis activities during the development of the conceptual design to address the known issues/constraints driven by information available at CD-0),
- preliminary environmental strategy (expected NEPA strategy, waste minimization/pollution prevention strategies, etc.),
- organizational interfaces,
- project risk analysis (cost, schedule, mission impact).

In addition to the three specific deliverables, a Mission Need Independent Project Review is required as part of the CD-0 ESAAB process. The DOE Office of Management, Budget, and Evaluation (OMBE) performs this function in coordination with the DOE Office of Engineering and Construction Management (OECM). Specific requirements are contained in the Mission Need and Critical Decision 0 Standard Operating Procedures dated February 23, 2004.

5.3.4 CD-1: Approve Preliminary Baseline Range:

Purpose: Selection of the best alternative solution at the conclusion of the concept exploration process. CD-1 establishes a baseline for design activities and authorizes use of preliminary engineering and design (PE&D) capital funding for the next phase of development, referred to as preliminary design.

Project Management: The Definition (CD-1) Phase involves the iterative process of developing and analyzing the concepts and alternatives available for meeting the mission need. The main activity that takes place leading up to CD-1 is development of the conceptual design and the generation of the Conceptual Design Report (CDR).

Supporting tasks include requirements and alternatives development and analysis, further development of the acquisition strategy, evaluation of project risks, hazards analysis, systems engineering, and value management/engineering. Additionally, the project develops a Preliminary Project Execution Plan that serves as a contract between NNSA and the Contractor for the execution of the next phase of the project. Completion of the CDR will also establish a baseline for remaining design activities (Preliminary and Definitive, or Title I and Title II).

NEPA documentation is usually initiated during this phase (preliminary environmental strategy including NEPA starts at CD-0) and requires input from the Preliminary Hazards Analysis, and the program Functional and Operational Requirements (F&OR) documents. Performance measurement during this phase

is assessed against the plan established for the Conceptual Design activities at CD-0. Critical Project Management requirements related to CD-1 are as follows:

- requirements that form the basis for the design and engineering phase of the project shall be clearly documented;
- a CDR shall be developed that includes a clear and concise description of the alternatives analyzed, the basis for the alternative selected, how the alternative meets the approved mission need, the functions/requirements that define the alternative, and demonstrates the capability for success;
- an acquisition strategy that accounts for risks and mitigation strategies shall be developed and reviewed by OMBE; and
- a value management assessment shall be conducted to determine formal value engineering study requirements.

5.3.5 Safety Analysis and Documentation:

During the conceptual design phase, which commences after receipt of CD-0, safety/safety basis activities are focused on identification and analysis of the hazards associated with the various alternatives to meeting the mission need with sufficient understanding to categorize the proposed project (include results to support propose or recommended alternative). The CDR (prepared during conceptual phase activities and approved as part of CD-1) establishes the design baseline. Safety analysis/documentation activities required to support the CD-1 – Approve Preliminary Baseline Range as illustrated in attachment II include:

- a. Finalize facility hazard characterization (e.g., inventories, forms, etc.), with emphasis on characterizing major hazards that will drive design requirements.

Example: From the pre-conceptual planning phase it was determined that at least 2 kg of ^{238}Pu is needed to produce qualified RTGs, the radioactive material will have to made extremely dispersible (i.e., well below respirable sizes - $<10\ \mu\text{m}$) in order to meet the design specifications for the RTGs (i.e., meet qualifications). ^{238}Pu tends to be highly- pyrophoric at this particle sizes in metal powder forms. In other words, we know that the major hazards are the presence of ^{238}Pu in highly dispersible forms, with the potential for fires from such activities.

- b. Final hazard categorization for the facility, based on unique facility characteristics associated with facility segmentation and/or hazardous material forms.

Example: Since the radioactive material needed to support the mission not only exceeds the HC-2 threshold for ^{238}Pu in DOE-STD-1027, but also it is highly dispersible and reactive in metal form (prior to oxidation and sintering) the final hazard categorization for the facility and operations still remains HC-2. Note that once ^{238}Pu is oxidized, the material becomes more chemically stable and not pyrophoric. Even though, it still has a high specific heat content.

c. Finalize facility siting determinations

Example: The evaluation of the impact of the facility siting on public, and adjacent facilities and worker personnel is completed for each design option (if require different sites), to determine if adequate protection can be provided to both workers and public. At this stage, the evaluation to determine if the proposed operations will adversely impact adjacent facilities and operations, or vice-versa has to be completed for all options.

Note: This output from safety/hazards analysis is also used as input to National Environmental Policy Act (NEPA) and other environmental/permitting analyses.

d. Completed impact assessment on safety for safety design exemptions

Example: At the end of the conceptual design phase, the seismic evaluation is completed including an assessment of the impact of seismic events including seismic induced fires on the future of this facility. A residual risk determination needs to be provided to the LASO Safety Authorization Basis Team Manager and LASO Manager for review and acceptance, respectively. Notice, that LASO Manager needs to get DOE approval prior to acceptance and implementation of an exemption to design requirements. The seismically induced Fire may also give some insight into other facility fires at this stage.

e. Preliminary or Design Hazard Analysis (PHA)

The PHA is started once the hazards have been identified and characterized. At this stage of the design phase (conceptual design) potential accident scenarios, and associated engineering controls are identified. Also, an assessment is made with respect to whether the defense-in-depth (DID) design concept is being met, and which are the most important DID controls. The basic outputs from a Hazards Analysis are:

- Defense-in-depth SSCs and preliminary safety functions, functional requirements, performance criteria.
- Safety Significant SSCs and preliminary safety functions, functional requirements, performance criteria.
- Which accidents screen in for full Accident Analysis

Additional considerations or details concerning the typical analysis or products of the PHA include the following:

- 1) Identify potential accident scenarios and consequences for major hazards identified, with focus on those scenarios that will drive design requirements.

Example: It is clear from the hazards that will be present within the facility, that operational accident scenarios associated with fires and loss of confinement (i.e., spills) will have to be identified as a minimum. Also, natural phenomena and external events that may result in releases from the facility will have to be identified including; these will include among

others seismic and high-wind events, and airplane crash events. Use bounding source and consequence calculations (typically back-of-the-envelope) to support the consequence estimates for each of the postulated accident scenarios.

Complete identification of facility engineering defense-in-depth controls (if possible process SSCs, to the extent information is available). *The PHA will identify the complete set of SSCs required to protect the workers and the public from potential uncontrolled releases based upon the level of information available at this stage, it also identifies many of the SSCs that will perform a safety-significant (SS) function (both because of their role in defense-in-depth and worker safety). Per DOE-STD-3009, the Hazard Analysis (HA) also gives some preliminary insight into SSC including identification of its preventive or mitigative safety functions(s) as determined in the hazard analysis (the Accident Analysis is not available for this yet). The HA may also yield preliminary information for some functional requirements. Functional requirements should be limited to those requirements necessary for the defined SSC safety function. Functional requirements are provided for safety-significant SSCs for the specific accident(s) or general rationales for which the SSC is needed (e.g., if that accident is not initiated by an earthquake, the functional requirement does not involve seismic parameters). Preliminary information may also become available from the HA scenario descriptions relative to performance criteria imposed on the safety-significant SCC so it can meet functional requirement(s) and thereby satisfy its safety function. Performance criteria characterize the specific operational responses and capabilities necessary to meet functional requirements. Safety-significant SSCs, are not required to consider performance criteria traditionally associated with safety-class SSCs or traditional nuclear standards in general. Performance criteria for safety-significant SSC should be representative of the general rigor associated with non-nuclear power reactor industrial and OSHA practices. Performance criteria for safety-significant SSCs are developed by DSA preparers using engineering judgment based on the expected functions for which it was designated a safety-significant SCC and its over all importance to safety.*

Example: Depending on the specific postulated accident scenario, all controls that are being planned to be included in the design of the facility are identified. For an operational fire, besides the previously identified safety SS-SSCs (i.e, facility structure), the following defense-in-depth SSCs and SS-SSCs could be identified (SS-SSCs are highlighted):

- *Glovebox confinement for operations with dispersible ²³⁸Pu (safety function at SS-SSC level is as a barrier to protect workers from large doses).*
- *Ventilation system (including HEPA filters and active ventilation) (as a required system for Gloveboxes to be operable, this would be a SS-SSC, safety function would be to ensure adequate delta-P across GBs to prevent to the spread of contamination).*
- *Fire suppression and detection system (Safety function would be to detect fires for fire department and facility notification/action, fire suppression would be to control fire progression).*
- *Inert capability for GBs (at least for those in which the potential for fire initiating is present) (Safety function is to limit oxygen available to prevent pyrophoric reactions and fire).*

- *Radiation monitors (safety function is detecting potential releases to working areas)*
- *Facility segmentation and fire zones (fire rated) to prevent fire propagation between facility areas.*

From these identify those controls that provide a SS function to prevent or mitigate a potential release from the postulated fire scenario, e.g., fire suppression system, HEPA filters.

- 2) Identify preliminary set of design basis accidents (DBAs) for the facility based on the potential for challenging or exceeding the EGs.

Example: *It is clear from the exemption and hazards identified that as a minimum DBAs covering seismic events (including seismic induced fires), operational fires, and loss of primary confinement (due to the presence of highly dispersible radioactive (i.e., ^{238}Pu) material). Other potential DBAs (bounding scenarios) need to be identified as part of the PHA based on the potential for other accident scenarios to challenge or exceed the DOE EG of 25 rem to the MOI. The completeness of the DBAs should at least cover all accidents that could drive the identification and design requirements for the facility SSCs; operational or process SSCs may or may not be included at this stage.*

- 3) Identify safety-class SSCs for DBAs that challenge or exceed the EG, based on the unmitigated consequences.

Example: *Based on the results of a quantitative analysis of the consequences for each of the DBAs, and the fact that the EG are exceeded for operational fires involving RTGs, the following SSCs designated as SC:*

- *Facility (structural and fire rating)*
- *HEPA filters (with maximum leak-path factor (LPF) for HEPA and facility confinement)*
- *Fire suppression system (since its failure may result in all inventory to be at risk, and confinement capabilities, e.g., LPF may be challenged)*

It is possible for some of these or other previously identified SS-SSCs to change safety designations, as the safety analysis matures and new information is incorporated into the analyses.

- 4) Establish some functional requirements for all facility (and to the extent possible for process equipment) safety SSCs (SC/SS-SSCs). *While the safety function is the top-level reason for designating safety SSCs (derived from the hazard analysis); the functional requirements define design requirements necessary to support the safety functions associated with SC and SS-SSCs. The functional requirements are identified by the accident analysis for SC-SSCs; while, for SS-SSCs can be derived from the hazard analysis.*

Example: *Functional requirements are typically associated with design criteria. For example, since seismically induced fires and seismic fires are likely to challenge or exceed the EG, the facility structure functional*

requirement is that it must meet PC-3 seismic design loads. Similar functional requirements can be derived for other SC/SS-SSCs.

- f. Update design requirements for facility SSCs, including criteria for integration of safety into the design

Example: *During the pre-conceptual planning phase and from the PHA during the conceptual design phase, it was concluded that the facility must meet PC-3 requirements since its failure could result in exceeded the DOE EG. The design requirements at this stage are translated into design specifications or performance requirements that will ensure that the functional requirement will be met. These performance requirements are typically measurable criterion that is associated with functional requirements and are derived from the accident analysis for SC-SSCs based on the environmental conditions that are generated by postulated DBAs. For hazard category 3 (HC-3) facilities or operations in which an accident analysis is not required, the performance requirements for SS-SSCs can be derived indirectly from the hazard analysis.*

For example, at LANL a PC-3 seismic event is expected to create static and dynamic loads with accelerations of the order of 0.3g. As such, the expected performance requirement for the structure is to be able to survive a 0.3 seismic event. Notice that a PC-3 seismic load at LANL is different than a PC-3 load at LLNL.

- g. Identification of all Codes and Standards completed for all facility SSCs

Example: *As indicated previously, DOE O 420.1 identifies facility safety design requirements (including codes and standards) in the areas of nuclear safety design, criticality safety, fire protection, natural phenomena hazards mitigation, and system engineering for all major modifications and new facilities. For the conceptual design phase, all of the codes and standards applicable to all of the facility SC- and SS-SSCs are identified.*

- h. The PDSA process is formally started with the preparation and completion of the design or preliminary hazard analysis. *As indicated in Section 5.3.2.4, the PDSA/PHA is submitted as part of CD-1 for review and approval.*

Example: *At this stage, the PDSA is focused on identification of safety SSCs and initial conditions assumed for the operation of the facility (i.e., maximum inventory of radioactive material). In other words, at this stage the PDSA is of the form of a PHA, the PHA includes all of the safety analyses above mentioned. .*

- i. Integrate safety with design document package, e.g., conceptual design report (CDR), facility and systems design descriptions (FDD/SDD)

Example: *The integration of safety into the design process starts from initiation of the definition or conceptual design phase. Any preliminary results of the PDSA/PrHA with respect to the identification of safety (emphasis on active) SSCs, safety functions, and other information important to the design of SSCs are documented in parallel in the design*

document package. Such design document package includes among others, conceptual design report (CDR), and the FDDs and SDDs as identified in Figure 2.

Integration of safety information that supports the design of safety SSCs is subjected to formal change-control procedures from the initiation of the project. Notice that as indicated in Figure 2, the PDSA and the results of the safety analysis drives the design requirements and thus the information to be documented in FDDs/SDDs and implemented during the design phases (preliminary/detail design).

All safety analysis and documents (including seismic evaluations, fire hazard analyses, etc.) shall be consistent with the design documentation, during the entire project management process.

At the end of the conceptual design phase, a complete PHA documenting all of the above safety analyses and information (including any safety analyses performed as part of the CD-0 activities) is provided as part of the CD-1 package.

- j. Design package and documents (e.g., FDD/SDD under change control) integrated with PHA/PDSA.

Summary of Safety Analysis and Documentation at CD-1:

At the end of the conceptual design phase (signaled by submittal of the Critical Decision 1 documentation package) the preliminary documented safety analysis (PDSA) in the form of a preliminary (design) hazard analysis is completed and submitted with the following safety basis information known/available to support the initiation of preliminary design phase activities:

- Completed facility hazard identification and characterization
- Final hazard categorization
- A comprehensive hazard analysis that will include a complete set of accident scenarios that will impact design and their associated defense-in-depth and SS-SSCs
- Complete identification of DBAs that will drive facility design requirements
- Relatively complete identification of major facility SC and SS-SSCs (note: SS-SSCs come from the HA not the AA), with the understating that some of these SSCs may change safety designation as the design progresses
- As complete a set of functional requirements for the SC-SSC and SS-SSCs identified as reasonably possible at this time based on the data available.
- Determined set of design requirements for any SC-SSCs and SS-SSCs, from those design requirements identified in DOE O 420.1 and its implementation guides
- Provide a complete evaluation of impacts (e.g., on safety of workers, public) of exemptions to design requirements, and identify preliminary design compensatory measures (if any). If such compensatory measures will be administrative controls, the PHA will need to provide a basis for determining the residual risk for full implementation and exemption cases
- At this stage not all DBAs and SC/SS-SSCs may be identified and evaluated. As the design matures (during CD-2/CD-3), changes may lead to changes to safety

designation or design requirements for SC/SS-SSCs. Also, additional information for process equipment will be integrated into the safety analysis process.

Figure 3 identifies the major ISM elements and their integration into the conceptual design (definition) phases. The ISM activities associated with defining the work (design baseline), design basis/analyze the hazards, develop design requirements, and perform design work (facility level) that were briefly discussed above are required to be completed during CD-1.

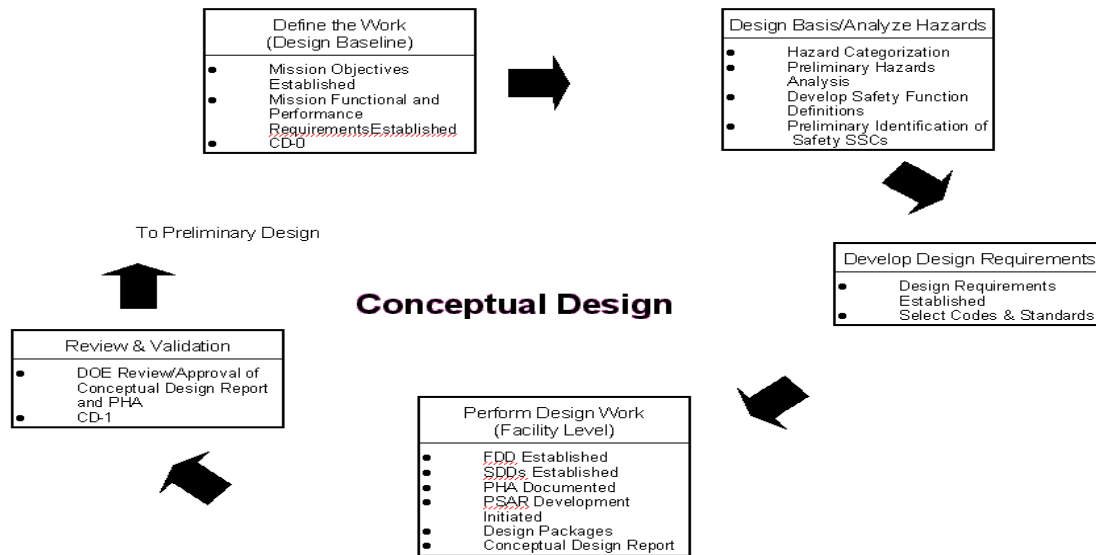


Figure 3. ISM Activities Associated with the Conceptual Design (or Definition) Phase

5.3.6 Deliverables: A CD-1 package consists of the following:

1. Acquisition Strategy (updated, with supporting documentation for recommended alternative)
2. Conceptual Design Report (CDR). The CDR will have the results of the PHA integrated, and consistent with other design documentation, e.g., seismic evaluations, FDDs/SDDs, fire hazard analyses, etc.
3. Preliminary Project Execution Plan and baseline range
4. Project Data Sheet for Design (identifies funding requirements to support Congressional Budget Request)
5. Verification of Mission Need
6. Preliminary Hazard Analysis Report completed (Preliminary Documented Safety Analysis at this phase of the project)

Also at this stage of the design process, preliminary NEPA assessments are completed, including identification of any permitting requirements, and waste minimization plans. The NEPA documentation needs to be also integrated with the SB documentation at the completion of the conceptual design phase. Any differences between these documents should be clearly documented and mostly related to analysis approaches, i.e., bounding analysis in the SB documentation versus, best estimates for NEPA documentation.

5.4 Facility/System Design Descriptions

- 5.4.1** A key tool used for documenting results of safety analysis and in particular the safety function, functional and performance requirements from the PDSA (PHA at this stage) are the Facility and System Design Description (FDD/SDD) documents. The FDDs/SDDs also support the integration of the safety analysis and the SB documentation. In other words, the PDSA is the basis for the development of the FDDs/SDDs. FDDs/SDDs shall be developed in accordance with DOE STD 3024-98, dated October 1998.
- 5.4.2** The FDD provides an overview of the relationship and interfaces of the various systems, structures and components that comprise the facility or plant. It is intended to present a concise summary of the design and principal parameters of the overall facility or plant as well as define the individual systems, facilities and services. In the FDD, all the systems in a facility can be addressed with their top-level functions and requirements with the more detailed information on those systems contained in the SDDs. FDDs are also the primary mechanism for addressing simple, less important systems such as potable water system, without having to develop SDDs for these types of systems.
- 5.4.3** An SDD identifies the requirements associated with SSCs, explains why those requirements exist (basis for the requirements), and describes the features of the system design provided to meet those requirements. As part of the configuration management change control process, the SDD helps to ensure consistency among the engineering requirements for the systems, the actual installed physical configuration, and the associated documentation. The SDD is a central coordinating link among engineering design documents, the facility authorization basis, and implementing procedures.
- 5.4.4** SDDs do not originate or drive requirements or authorization/safety-basis information, but rather collect that information into a convenient, useable form. The SDD is intended to consolidate information regarding a particular system into one document. FDDs/SDDs are not authorization basis documents, yet they support this function and help ensure operations of a system or facility, are within the approved authorization basis. F/SDDs should be controlled documents and maintained as up-to-date authoritative sources of technical information.
- 5.4.5** During design and construction of new facilities, the F/SDDs serve as the vehicle for collecting and conveying system requirements and their bases (i.e. technical baseline). F/SDDs should contain requirements derived from both programmatic needs as well as from safety analysis. Requirements that feed F/SDDs should flow down from the mission need statement, through program requirements documents, functional and operation requirements documents, design criteria, hazards analysis, and documented safety analysis documentation. SDD information should flow from and be tiered off of FDD information.
- 5.4.6** As part of the pre-conceptual planning, decisions must be made regarding development of F/SDD's based on the initial facility/hazard categorization driven by information contained in the mission need statement. Normally, Hazard Category 2 facilities will require SDD's be developed for all SC/SS SSCs, with an FDD developed for the balance of

the facility. For Hazard Category 3 facilities, it may be decided that separate SDDs not be developed, but rather an FDD would be developed that describes the overall facility and summarizes the various SSCs.

5.4.7 F/SDD's are initiated after CD-0 as part of the conceptual design and are normally contained as a section of the Conceptual Design Report. At CD-1, the F/SDD is essentially outline form with information developed as much as possible given the level of hazards and safety analysis available at this point in the project. As noted in 5.4.5 above, F/SDDs serve to collect information that is produced and derived through design evolution and safety basis development. At each subsequent state of project development, the F/SDDs will become more and more detailed, summarizing results of continued maturation of design and safety basis development.

5.4.8 As with the FDDs/SDDs and SB documentation, all other design and safety analyses and documentation needs to be maintained updated and consistent with each other at the time of being submitted as part of a CD document package.

5.5 Change Control

DOE O 413.3 Chapter II provides specific requirements for baseline change control within the project management functional area. From a project management perspective, change control ensures that project changes (cost, schedule and technical scope) are identified, evaluated, coordinated, controlled, reviewed, dispositioned, and documented in a formal manner. Formal baseline change control processes are required for design activities on projects after CD-1, with specific processes and thresholds for change control described in the individual Project Execution Plans (PEPs), tailored for each individual project.

Change control requirements applicable to safety basis requirements are contained in DOE O 420.1A, Chapter 4, Section 4.5.1.2, Configuration Management. This chapter of 420.1A also references use of DOE-STD-3024-98, *Content of System Design Descriptions*, as primary guidance on identification and consolidation of key design documents necessary to support 10 CFR 830 Subpart B documentation requirements.

Project planning and development activities initiated during the pre-conceptual and conceptual design phases produce the technical, cost, and schedule baseline information necessary to establish a design baseline and ultimately, a performance baseline for the overall project at CD-2. This baseline information is contained in a variety of project documents including, but not limited to the Mission Need Statement, Program Requirements Document, Conceptual Design Report, and the Preliminary Hazards Analysis. As baseline information is developed and established on a project, formalized change control processes must be implemented in accordance with DOE O 413.3 and DOE O 420.1A requirements.

At the completion of conceptual design phase activities, formal change control processes to be applied on each project during the remainder of design phase activities shall be described in the Preliminary Project Execution Plan (PPEP), a specific CD-1 deliverable. At CD-1, a formal baseline for design activities is established for which formal change control processes will be applied. As the PHA represents the PDSA at CD-1, the PPEP shall also address change control

requirements applicable to the further development of the PDSA during design phase activities. In other words, the PPEP should not only address the traditional change control thresholds for project technical, cost, and schedule parameters, it should also contain thresholds for key safety-basis parameters identified during PHA development.

Specific goals of the change control process articulated in the PPEP at CD-1 include:

- Anticipate, recognize, and predict changes
- Prevent performance baseline deviations
- Evaluate, and understand the impacts of each change
- Identify, understand, and control the consequences of changes
- Prevent the unauthorized or unintended deviations from approved baselines
- Ensure each change is evaluated, reviewed, and dispositioned at the proper management level

After approval of the mission need (CD-0), all deliverables associated with CD packages over the life of a project should have consistent safety basis documentation (PDSA/DSA) and FDDs/SDDs. That is, the FDDs/SDDs should reflect the same level of development as that reflected in the SB documentation.

6.0 RECORDS

Records packages generated by this procedure shall be maintained as QA records, and must be identified as such by the originator.

7.0 ATTACHMENTS

7.1 Attachment I DOE Order 413.3 Project Acquisition Process And Critical Decisions

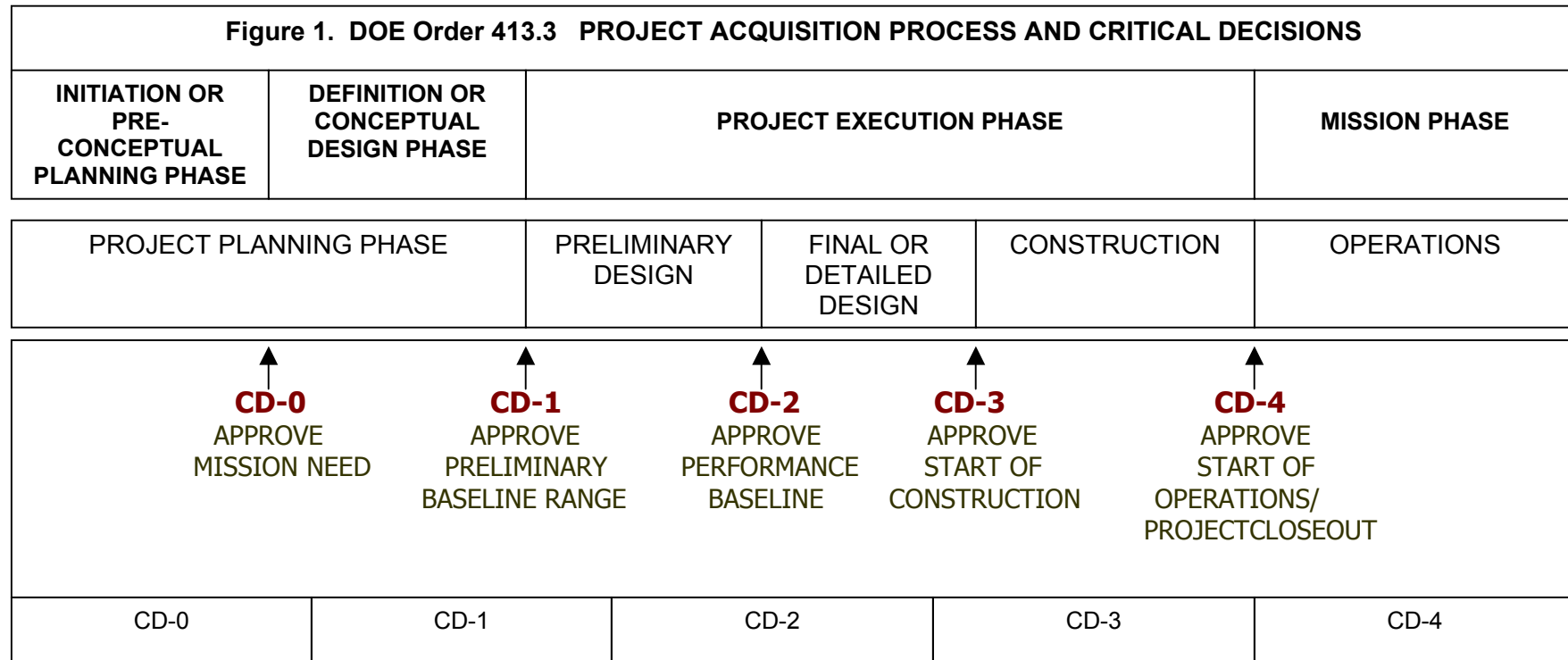
7.2 Attachment II Figure 2. NNSA-LASO Safety-Design Integration Process Flow

8.0 REVISION HISTORY

8.1 Revision 0 – New Procedure

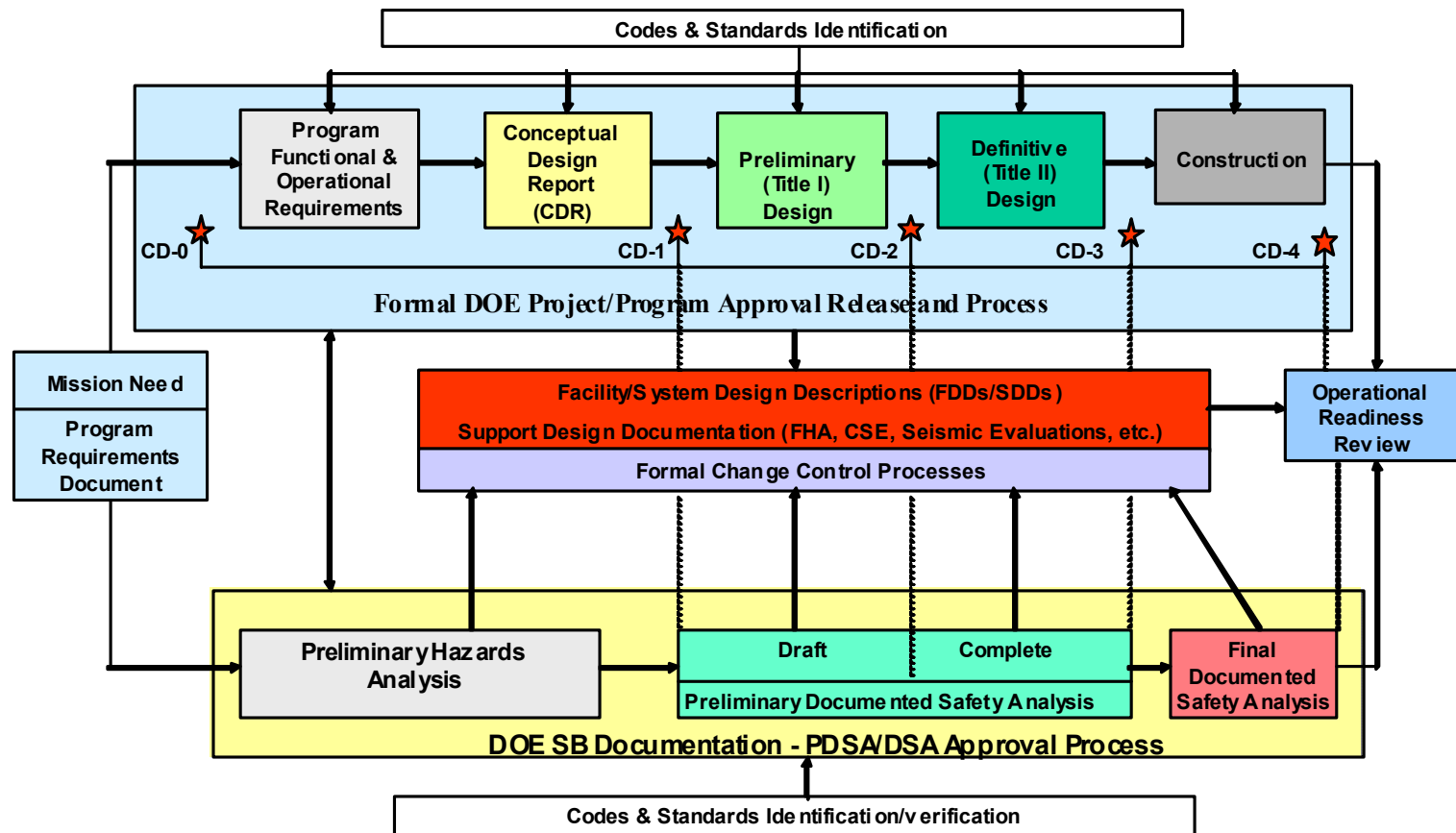
Attachment I

DOE Order 413.3 PROJECT ACQUISITION PROCESS AND CRITICAL DECISIONS



Attachment II






NNSA-LASO Safety-Design Integration Process Flow



Project Management development cycle (Planning/Design/Construction) per DOE Order 413.3

DSA Development cycle per DOE Order 420.1, and DOE Guide 421.1-2

Table 1. Integration of ISM Activities i

Function	Ensure project procedures require development of products DOE expects at the proper time				
	Conceptual Design	Preliminary Design	Detail Design	Construction	
Define the Work (Design Baseline)	Mission Objective Established Mission Functional and Performance Requirements Established CD-0	FDD Under Change Control SDD Under Change Control CDR Establishes Design Baseline	SSC Design Requirements Under Change Control FDD & SDDs Under Change Control Title I Design Report Established Design Baseline	PDSA and SER Under Change Control Detailed Design Under Change Control FDD and SDDs Under Change Control	
Design Basis/ Analyze Hazards	Hazard Categorization Preliminary Hazards Analysis Develop Safety Function Definitions Preliminary Identification of Safety SSCs	Process Hazards Analysis Mostly Complete Design Basis Accident Identified Safety Functions Finalized Identification of Safety SSCs Complete	Analysis Complete Accident Analysis Completed and DBAs Fully Established Safety SSC Functional Requirements Finalized SSC Performance Requirements Fully Defined	Effects of Changes During Construction are Analyzed for Their Effect on Safety PDSA Updated and Finalized Accident Analysis Updated and Finalized	
Develop Design Requirements	Design Requirements Established Identify Codes and Standards	Safety SSC Functional Requirements Established Design Reqts Updated Codes/Standards Updated	Design Reqts Finalized Codes/Standards Finalized Procurement Specifications are Prepared	TSRs Developed Consistent With Design Construction Safety Following ISM	
Design Work	FDD & SDDs Established PHA Documented PDSA Development Initiated Design Packages Developed Conceptual Design Report	FDD and SDDs Updated Draft PDSA Established Design Packages Updated Title I Design Report	FDD and SDDs Updated PDSA Complete Detail Design Packages Finalized Title II Design Report	FDD and SDDs are Completed As-built Drawings Developed DSA Developed and Finalized	
Review & Validation	DOE Review/Approval of CDR and PDSA (PHA) CD-1	DOE Review/Approval of Title I Design Report Draft PDSA Reviewed CD-2	DOE Review/Approval of Title II Design Report DOE Review/Approval of PDSA (SER) Feedback to contractor WSS CD-3	(SER) FDD, SDDs, As-builts as Controlled Documents that Control Safety Features Feed-in to contractor WSS Confirm Readiness to Operate, Transition to Operations, CD-4	
	 CD-0	 CD-1	 CD-2	 CD-3	 CD-4